多年区块链交易系统产品研发实践经验的概括和总结
助你快速设计搭建一个属于自己的区块链交易系统

Broadview
www.broadview.com.cn

区块链
交易系统开发指南

武源文 柏罡 温江凌 著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

区块链
交易系统开发指南

武源文 柏罡 温江凌 著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书使用通俗易懂的语言，从技术的角度详细介绍了区块链交易系统应有的功能架构及工作原理，让人们能够张开双臂轻松地拥抱区块链技术，享受区块链交易系统带来的惊喜与成就感。

本书共分 7 章，第 1~2 章主要介绍区块链及数字货币的基本概念，以及各种公有链的 API 接口；第 3~5 章主要介绍区块链交易系统的分类架构及功能；第 6 章主要介绍区块链交易系统面临的问题及演进方向；第 7 章对全书做了总结。

本书是作者多年从事区块链交易系统产品研发实践经验的概括和总结，实用性和技术指导性较强，可供从事区块链产品研发和区块链交易系统研发的人员参考研究，也可供希望了解区块链技术或希望投身于区块链交易系统开发的技术人员学习。本书同样适用于传统行业、互联网金融等一些非区块链行业中从事电子商务、在线购物等其他交易系统产品研发、测试、维护等的技术人员参考学习。

图书在版编目（CIP）数据

区块链：交易系统开发指南 / 武源文，柏罡，温江凌著. —北京：电子工业出版社，2018.10
ISBN 978-7-121-35007-8

Ⅰ. ①区… Ⅱ. ①武… ②柏… ③温… Ⅲ. ①程序设计 Ⅳ. ①TP311.1

中国版本图书馆 CIP 数据核字（2018）第 207740 号

策划编辑：董　英
责任编辑：葛　娜
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×980　1/16　　印张：19.25　　字数：384 千字
版　　次：2018 年 10 月第 1 版
印　　次：2018 年 10 月第 1 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

序

交易（transaction）是最基本的经济活动，也是区块链中最基本的数据结构。我当初学习比特币技术的时候，对比特币中的transaction数据结构设计狠下过一番工夫进行研究。然而，比特币中的交易是单向的，只包含了资金侧的转账支付（transfer/pay），并不包含商品和服务流一侧的数据。在理想的通证经济系统中，交易的双侧都应该表达为通证的流转，也就是代表价值的通证与代表商品与服务权益的通证在交易中进行原子化的所有权对调（exchange）。

麻烦的是，在中文区块链世界里，我们把 transaction 翻译成“交易”，把 exchange 也翻译成“交易”，这就摆了乌龙。实际上，transaction 在数据库技术世界中被普遍翻译为“事务”，强调的是其原子性——要么保持原状，要么完全成功，没有中间状态。在 transaction 中既包括 transfer/pay，也包括 exchange，还可以有其他更复杂的操作，因此在区块链世界里，将 transaction 翻译成“交易”是不合适的。交易，要有来有往，有交有易。所以，exchange 才是交易。

支付（transfer/pay）是单向的，而交易（exchange）是双向的。通证经济的基础设施，将会努力将各种价值和权益都通证化，因此在通证经济中交易表现为两份通证的对换。你去电商网站购买商品，其实花出去的是数字货币，买到的是一张数字合同，这才是这次交易的本质。至于商家通过快递将商品发送给你，只是对数字合同规定条款的履约行为，是“副作用”。

单向的通证流转（transfer/pay），以及双向的通证对换交易（exchange），这是未来通证经济中最基本的两个事务性操作。后者当然要比前者复杂，但由于包含了完整的交易流

信息，因此可以更好地进行验证、追溯、分析和优化，其价值要比前者高得多。

理解了这一点，我们就会明白，在未来的大多数通证经济应用场景下，交易（exchange）将成为最普遍的基本操作。在通证经济里，购物是交易，阅读是交易，发表文章是交易，投票是交易，可能说句话都是交易。我们甚至可以把本来是支付的操作升级为交易——用户的支付行为，实际上是用一笔数字资产交换一个数字收据。这样一来，我们也可以认为，未来的世界，交易将是泛在（pervasive）的。

然而，看看我们现在的区块链和通证技术圈子，交易这一操作只集中出现在一个场所中，那就是交易所。而在其他大部分区块链和通证经济应用中，都回避了双向的 exchange，而钟情于单向的 transfer/pay。在这样的架构下，从区块链上你只能看到交易的一半，看不到另一半。这显然不能被视为通证经济的高级状态。

我在这里大胆猜测，未来在每一个区块链和通证经济应用当中，都需要有交易系统的功能，或者内置，或者外包，或者服务化，总之，交易系统将无所不在，集合竞价的交易模式将无所不在。

也就是说，未来当通证经济发展到成熟阶段的时候，交易系统将不独为某一类特别组织所有，而是泛在的基础设施。交易系统技术将成为与 Web 后端一样被广泛研究的技术，数以百万计的开发者将会在这个领域工作。因此，学习和研究交易系统技术，对于今天的技术人员来说，绝对是最具价值的投资之一。

遗憾的是，交易系统开发绝非易事，不但涉及面广，而且在性能、并发、安全等核心技术上有极大的挑战。更糟糕的是，市面上探讨交易系统开发技术的资料十分稀缺，高质量的内容更加少见。

由井通生态团队编写的这本开发指南，几乎是目前市面上唯一一本从开发技术层面阐述交易系统的图书，可谓本类作品的一个起点。可贵的是，这个起点相当高，这本书不但内容丰富，覆盖了区块链交易系统的各个方面，而且特别“实诚”，可谓“刀刀见肉”，章章都是实料。我本人并非这个领域的专家，但是翻读此书，对于交易系统的认识有了很大的提升。如果读者是一位有经验的开发者，那么这本书应该可以引导他走入区块链交易系统开发的大门。

很愿意向技术圈的朋友推荐这本书，我相信这本书会在中国区块链和通证经济的发展进程中留下自己的印记。

孟岩

前　言

在区块链问世的第 10 个年头，区块链和区块链技术已经越来越多地出现在我们的生活中，越来越深入地改变着我们的价值传递方式。区块链交易系统可以为价值传递提供安全、可靠、便捷的活动场所，因此也逐渐受到人们的青睐。而如果没有系统地研究学习过区块链，则很容易被各种抽象概念和复杂的设计理念搞得云里雾里摸不着头脑。若要想设计搭建一个属于自己的区块链交易系统，更是无从下手。本书使用通俗易懂的语言，介绍了区块链的基本概念、设计思想，并从技术的角度详细介绍了区块链交易系统应有的功能架构及工作原理，目的就是揭开区块链交易系统的神秘面纱，填坑清障，指引前行，让人们能够张开双臂轻松地拥抱区块链技术，享受区块链交易系统带来的惊喜与成就感。

本书共分 7 章，第 1~2 章主要介绍区块链及数字货币的基本概念，以及各种公有链的 API 接口；第 3~5 章主要介绍区块链交易系统的分类架构及功能；第 6 章主要介绍区块链交易系统面临的问题及演进方向；第 7 章对全书做了总结。王春、王万云、王亚伟、魏庆伟、潘子鑫、郝运锴、张庆娜等协助本书作者完成了大量的资料收集和整理工作，计松辰对全书内容进行了统稿。

本书是作者多年从事区块链交易系统产品研发实践经验的概括和总结，实用性和技术指导性较强，可供从事区块链产品研发和区块链交易系统研发的人员参考研究，也可供希望了解区块链技术或希望投身于区块链交易系统开发的技术人员学习。本书同样适用于传统行业、互联网金融等一些非区块链行业中从事电子商务、在线购物等其他交易系统产品

研发、测试、维护等的技术人员参考学习。

在本书出版之际，衷心感谢张少华、李孟杰、郭媛媛、王春、王栋、韩金祺、赵树理等与我们分享了运营实践、产品架构设计等多个层面的丰富经验，并为本书的编写提出了非常宝贵的意见和建议；感谢在本书编写过程中给予我们大力支持和帮助的各界人士；感谢电子工业出版社的大力支持。在本书编写过程中参考了大量的文献资料，对这些文献资料的作者表示真诚的谢意。

由于水平有限，书中难免出现纰漏和不妥之处，敬请读者朋友们批评指正。

读者服务

轻松注册成为博文视点社区用户（www.broadview.com.cn），扫码直达本书页面。

- **提交勘误**：您对书中内容的修改意见可在*提交勘误*处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **交流互动**：在页面下方*读者评论*处留下您的疑问或观点，与我们和其他读者一同学习交流。

页面入口：http://www.broadview.com.cn/35007

目　录

1

第 1 章

区块链交易系统基础

1.1 区块链概述

1.1.1 区块链的定义

区块链技术是构建价值互联网不可或缺的底层应用技术，是具备多级层和多类型应用的价值传输技术的集合。它的本质是一种分布式数据库，或者说是一个可共享且不易更改的分布式分类总账。

该技术方案让参与系统中的任意多个节点，把一段时间系统内的全部信息数据，通过密码学算法计算和记录到一个数据块即区块中，并生成数据“密码”用于验证其信息的有效性和链接下一个数据块，并且由系统的所有参与节点来共同认定记录是否为真。

现在让我们从区块链的起源来更深入地了解区块链。2008 年 11 月 1 日，正当金融危机席卷全球时，一位名叫中本聪的神秘人物向“密码学邮件组”发布了一个帖子：“我们正在开发一种新的电子货币系统，其采用完全点对点的形式，而且无需第三方信托机构。”这样一种不受任何政府或主权控制、去中心化的全球电子货币系统是“密码朋克们”数十年的梦想。

比特币的问世及稳定运行的10年证明了区块链技术对于价值传输的可靠性及安全性，开启了互联网由信息互联时代迈向价值互联时代的大门。

在中本聪发布的 *Bitcoin: A Peer-to-Peer Electronic Cash* 论文中，我们看到了这种电子货币体系的几项颠覆式创新。

（1）去中心化。比特币的发行和流通不依靠中央银行等第三方机构，而是依靠特定算法及密码学技术通过点对点的传输实现，是一种完全依靠网络节点的分布式虚拟货币。

（2）开源性。在比特币系统中，所有参与者都可以成为比特币的发行者及交易者，整个系统的运作规则是公开透明的，任何个人或机构都可使用比特币系统，整个系统是以开源的方式存在的。

（3）匿名性。在比特币系统中，任何个人或组织都可以开设比特币账户，而每个账户对应的地址实际上是与用户的现实身份没有任何关系的 ID。比特币持有者可通过不断转换 ID 来隐藏自己的身份。同时，整个比特币网络都不存储可以辨认个人身份的信息。

（4）不可逆性。全部交易都被加上时间戳，并将交易信息并入一个不断延展的基于散列算法的工作量证明的链条上作为交易记录。除非重新完成全部的工作量证明，否则所形成的交易记录将不可变更。

（5）安全性。公钥与私钥相结合。公钥用于计算比特币地址，而操控比特币需要私钥，它可以被隔离保存在任何存储介质上，除了用户自己无人可以获取。此外，系统中的每个节点都能获得一份完整数据库的拷贝，得知所有比特币的交易信息。除非同时控制整个系统中超过 51%的节点，否则在单个节点上对数据库的修改是无效的。因此，比特币的安全性将随着参与者的增加而提升。

（6）全球自由便捷流通。使用比特币没有烦琐的手续，只需要告知对方比特币地址就可进行支付。任何一台接入互联网的计算机都能被用来管理比特币。

从中本聪的这套点对点电子货币体系中我们可以看到区块链的雏形，即一种不依靠第三方而实现价值转移的分布式账本技术。这种账本具备以下几个特征。

- 无限扩展性：区块链上的每个区块都可被看作账本中的一页，在区块上记录着一条或多条交易信息，每增加一个区块就相当于账本增加一页，区块链上的区块数量是没有上限的。
- 全员维护：账本依靠网络中的节点共同记录与维护，不依靠第三方机构。
- 加密且有序排列：交易信息被加密打包和记录到每一个区块中，并加盖时间戳，一个个区块根据时间戳顺序链接成一个总账本。

在这里，我们必须要强调比特币并不等同于区块链，它只是区块链技术的一个早期的最典型的应用范例。这个应用范例的问世打开了区块链的“潘多拉魔盒”，让虚拟的互联网世界开启了价值互联的时代，其核心是依靠技术手段建立一种无需第三方担保的安全可信任的机制，让人人可以参与其中。

1.1.2　区块链的核心原理

区块链的核心理念是：构建前后关联且可相互验证的数据块（即区块），并通过时间戳将区块排序，结合密码学技术，形成集体维护、彼此验证、有序链接的网状价值传输系统。

关于区块链，我们需要理解几个核心概念。

1. 区块

在区块链技术中，有价值的信息以数据的形式被永久存储下来，这些用于存储数据信息的载体被称为区块。区块按时间顺序排列，每个区块都记录着它在被创建期间所发生的交易信息，所有区块有序链接起来以汇聚成一本“总账”，而每个区块都可被看作总账中的一页。

每个区块均包含三个要素：①本区块的 ID；②若干交易单；③前一个区块的 ID。

在比特币系统中，每隔 10 分钟创建一个区块，这个区块记录了在这段时间内发生的所有交易信息。同时，每个区块都包含前一个区块的 ID，因此便可根据此 ID 找到上一个区块，依此类推，追踪到起始区块，从而可以生成一个完整的交易链条，形成区块链。

2. 时间戳

顾名思义，时间戳是记录某一事件发生时点的信息。在区块链中从区块生成的那一刻

开始，时间戳便存在于区块中。由于时间的唯一性，让每个加盖了时间戳的区块都是独一无二的，并且提供了认证依据，保证了它的真实性。通过时间戳，各个区块有序排列起来，最后生成一个完整的链条。

3. 散列算法

散列算法是区块链中保证交易信息不被篡改的单向密码机制。区块链通过散列算法对一个交易区块中的交易进行加密，并把信息压缩成由一串数字和字母组成的散列字符串。区块链的散列值能够唯一而准确地标识一个区块。在验证区块的真实性时，只需要简单计算出这个区块的散列值，如果没有变化就意味着这个区块上的信息是没有被篡改过的。

4. 公钥和私钥

从密码学的角度定义，公钥和私钥其实是一种不对称的加密方式，其核心思想是加密与解密采用不同的密钥。在区块链中使用公钥和私钥标识身份，信息发送者用私钥对信息进行签名，使用信息接收方的公钥对信息加密；信息接收方用信息发送者的公钥验证发送者的身份，使用私钥对加密信息解密。

在介绍了区块链的核心原理和几个核心概念后，我们不难发现，区块链技术是密码学、经济学、分布式存储技术、网络科学及应用数据等多种技术的整合，目的是构建一套可信任的价值传输体系。这些技术按特定规则组合在一起，构建了一套分布式数据记录和存储系统，并通过时间戳为存储数据的区块排序，形成一个连续且前后关联的分布式数据库，这个数据库是价值的天然载体。

1.1.3 区块链的特性

与传统记账方式相比，区块链具有去中心化、开放性、自治性、集体维护、信息不可篡改、匿名性、可追溯性、智能性等特性。

1. 去中心化

区块链本质上是分布式数据库，因此区块链上的数据发送、验证、存储等均基于分布式系统架构，依靠算法和程序来建立可信任的机制，而非第三方机构。任意节点的权利和义务都是均等的，交易双方可以自证并直接交易，不需要依赖第三方机构的信用背书。同

时，任何一个节点的损坏或者退出都不会影响整个系统的运行。

2. 开放性

区块链系统是开放的，除交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用。

3. 自治性

区块链采用协商一致的规范和协议（比如一套公开透明的算法），使得整个系统中的所有节点能够在去信任的环境中自由安全地交换数据，使得对“人”的信任改成对机器的信任，任何人为的干预都不起作用。

4. 集体维护

区块链系统是由所有参与节点共同维护的系统。区块链上的每一个节点都可以对区块（数据块）进行维护，而整个系统的运行也依赖每一个节点，这是一个人人参与其中的集体维护系统。

5. 信息不可篡改

经过验证的信息被上传至区块链后就会被系统永久存储下来，并得到所有参与节点的集体维护。除非能够同时控制系统中超过 51%的节点，否则在单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

6. 匿名性

区块链上的信任体系由程序和算法构建，节点之间的交换遵循固定的算法。交易双方无须通过验证现实中的身份信息来让对方产生信任，因此匿名性是区块链很明显的一个特征。

7. 可追溯性

溯源是指追踪记录有形商品或无形信息的流转链条。在区块链上每一个区块都会被加盖时间戳。时间戳既标识了每一个区块独一无二的身份，又让区块实现了有序排列，为信息溯源找到了很好的路径。

8. 智能性

在以上 7 个特性的基础上，区块链还具备可编程性、可承载智能合约等技术。这个特性让人们可以根据具体的应用场景，在区块链上创建和部署相关程序，以实现智能化运行。

1.2 区块链分类

根据参与者的不同，区块链可以分为公有（Public）链、联盟（Consortium）链和私有（Private）链，如图 1-1 所示。

图 1-1

1.2.1 公有链

公有链，顾名思义，任何人都可以参与使用和维护，典型的如比特币区块链，信息是完全公开的。通常公有链也称为非许可链（Permissionless Blockchain），无官方组织及管理机构，无中心服务器，参与的节点按照系统规格自由接入网络，不受控制，节点间基于共识机制开展工作。

公有链是真正意义上的完全去中心化的区块链，它通过密码学保证交易不可篡改，同时也利用密码学验证结合经济上的激励，在互为陌生的网络环境中建立共识，从而形成去中心化的信用机制。公有链中的共识机制一般是工作量证明（PoW）或权益证明（PoS），用户对共识形成的影响力直接取决于他们在网络中拥有资源的占比。

公有链一般适合于数字货币、面向大众的电子商务，以及互联网金融等 B2C、C2C 或 C2B 等应用场景，比特币和以太坊等就是典型的公有链。